DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Robert Loyd on 4/20/2010.

In the claims:

1. (Currently Amended) A method for re-encrypting encrypted data in a secure storage file system, comprising:

obtaining one or more selected encrypted data blocks from the secure storage file system, each selected encrypted data block comprising a selected encrypted data,

the one or more selected encrypted data blocks comprising data blocks accessed by a first user, wherein the one or more selected encrypted data blocks were selected based on ~~using~~ a user data access record, wherein the user data access record comprises a bitmap indicating which encrypted data blocks ~~is~~ are accessed by a first user;

decrypting, re-encrypting and storing each one of the one or more selected encrypted data blocks, the decrypting, re-encrypting and storing of each data block comprising:

decrypting the selected encrypted data using a first symmetric key associated with the encrypted data block to obtain selected data;

re-encrypting the selected data using a second symmetric key associated with the data block to obtain new encrypted data;

for each user who has access to the data block,

obtaining a public key associated with a private key, wherein the first user is denied access to the private key;

encrypting the second symmetric key using the public key to obtain a new encrypted symmetric key;

storing in a new data block, stored in a storage device;

the new encrypted data and the new encrypted symmetric key if a second user has read permission, wherein the second user is allowed access to the private key;

applying a hash function to the selected data to obtain hash data;

encrypting the hash data with the private key to obtain encrypted hash data; and

storing the encrypted hash data, the new encrypted data, and the new encrypted symmetric key if the second user has write permission.

13. (Currently Amended) A computer system generating a secure storage file system, comprising:

a processor;

a memory;

a storage device;

a computer display; and

software instructions stored in the memory for enabling the computer system under control of the processor, to perform:

obtaining one or more selected encrypted data blocks from the secure storage file system, ~~using a user data access record, wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a first user~~

each selected encrypted data block comprising a selected encrypted data,

the one or more selected encrypted data blocks comprising data blocks accessed by a first user, wherein the one or more selected encrypted data blocks were selected based on a user data access record, wherein the user data access record comprises a bitmap indicating which encrypted data blocks are accessed by a first user;

decrypting, re-encrypting and storing each one of the one or more selected encrypted data blocks, the decrypting, re-encrypting and storing of each data block comprising:

decrypting the selected encrypted data using a first symmetric key associated with the data block to obtain selected data;

re-encrypting the selected data using a second symmetric key associated with the data block to obtain new encrypted data;

for each user who has access to the data block,

obtaining a public key associated with a private key, wherein the first user is denied access to the private key;

encrypting the second symmetric key using the public key to obtain a new encrypted symmetric key;

storing in a new data block, stored in a storage device the new encrypted data and the new encrypted symmetric key if a second user has read permission, wherein the second user is allowed access to the private key;

applying a hash function to the selected data to obtain hash data;

encrypting the hash data with the public key to obtain encrypted hash data; and

storing the encrypted hash data, the new encrypted data, and the new encrypted symmetric key if the second user has write permission.

20. (Currently Amended) A secure storage system comprising:

a storage provider storing encrypted data in a storage device, ~~wherein re-encrypting the encrypted data comprises~~:

obtaining one or more selected encrypted data blocks from the secure storage file system, each selected encrypted data block comprising a selected encrypted data, the secure storage file system executing on the storage provider using a user data access record in response to receiving a key re-encryption event, ~~wherein the user data access record comprises a bitmap indicating which encrypted data is accessed by a first user;~~

~~decrypting the selected encrypted data using a first symmetric key to obtain selected data~~;

the one or more selected encrypted data blocks comprising data blocks accessed by a first user, wherein the one or more selected encrypted data blocks were selected based on a user data access record, wherein the user data access record comprises a bitmap indicating which encrypted data blocks are accessed by a first user;

decrypting, re-encrypting and storing each one of the one or more selected encrypted data blocks, the decrypting, re-encrypting and storing of each data block comprising:

> decrypting the selected encrypted data using a first symmetric key associated with the encrypted data block to obtain selected data;

re-encrypting the selected data using a second symmetric key associated with the data block to obtain new encrypted data;

for each user who has access to the data block,

obtaining a public key associated with a private key, wherein the first user is denied

access to the private key;

encrypting the second symmetric key using the public key to obtain a new encrypted

symmetric key;

storing in a new data block, stored in the storage device, the new encrypted data and

the new encrypted symmetric key if a second user has read permission, wherein the

second user is allowed access to the private key;

applying a hash function to the selected data to obtain hash data;

encrypting the hash data with the private key to obtain encrypted hash data; and

storing the encrypted hash data, the new encrypted data, and the new encrypted

symmetric key if the second user has write permission; and

a client device, wherein the client device comprises a client kernel for generating the

key re-encryption event and a client application using the encrypted data.

30. (cancelled).

No other claim is further amended.

Response to Arguments

6. Applicant's argument relative to the rejections under section 112 in light of the amendments made in their response filed 2/24/2010 has been found persuasive. The rejections are hereby withdrawn.

Applicant's argument relative to prior art rejection in light of the amendments noted by this action, and the telephone interview conducted on 4/20/2010 have been found persuasive (please see the attached Interview Summary).

Allowable Subject Matter

7. Amended claims 1-7, 13-23 now re-numbered as claims 1-18 are allowed.

Examiner's Statement of Reasons for Allowance

8. The following is an examiner's statement of reasons for allowance:

None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed, particularly the feature of selecting data accessed by a user based on a bit map access record, decrypting all accessed data, and re-encrypting all the accessed data with a new symmetric key and encrypting the symmetric key using the

public key of each system user separately, and saving the encrypted symmetric keys encrypted using the public keys of each user in a separate data block along with the encrypted data, and depending on each user's read/write permission, also storing a hash of the accessed data in each data block, among other features of the independent claims.

Conclusion

9. Any comments considered necessary by the applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "comments on statement of reasons for allowance."

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Farid Homayounmehr/
Examiner
Art Unit 2439